12 FAM 590
CYBER SECURITY INCIDENT PROGRAM (SENSITIVE BUT UNCLASSIFED (SBU) SYSTEMS)

(CT:DS-116; 11-01-2005)
(Office of Origin: DS/IS/APD)

12 FAM 591 GENERAL

12 FAM 591.1 Purpose

(CT:DS-116; 11-01-2005)

a. The purpose of the Cyber Security Incident Program (CSIP) is to enhance the protection of Department of State's unclassified cyber infrastructure by identifying, evaluating, and assigning responsibility for breaches of cyber security.

b. The Department considers its unclassified cyber infrastructure to be sensitive. The confidentiality, integrity and availability of Department automated information systems (AISs) are critical to its operations. At posts abroad, the chief of mission (COM) is the ultimate owner of that portion of the Department's cyber infrastructure and is responsible for its security. Domestically, the Bureau Executive is considered the system owner (see 5 FAM 814 r). In both cases, system security functions are delegated to the information systems security officer (ISSOs). The program implements the Federal Information Security Management Act (FISMA) of 2002.

c. The CSIP focuses on accountability of personnel for actions leading to damage or risk to Department AISs and infrastructure, even when only unclassified material or information is involved.

12 FAM 591.2 Applicability

(CT:DS-116; 11-01-2005)

The CSIP applies to all Department AIS users. It pertains to the Department's unclassified systems. Therefore, employees who do not

possess security clearances also fall under its provisions.

12 FAM 591.3 Authorities

(CT:DS-116; 11-01-2005)

a. Relevant legal authorities include:

(1) Federal Information Security Management Act (FISMA)(2002);

(2) Computer Fraud and Abuse Act (1984), as amended by the United States of America Patriot Act of 2001;

(3) Privacy Act of 1974; and

(4) Executive Order 13231, Critical Infrastructure Protection in the Information Age (2001), February 28, 2003.

b. Relevant FAM sections include:

(1) 12 FAM 620, Unclassified Automated Information Systems;

(2) 5 FAM 700, Internet and Intranet Use; and

(3) 5 FAM 800, Information Systems Management.

12 FAM 592 CYBER SECURITY INCIDENTS

(CT:DS-116; 11-01-2005)

As it relates to this program, a "cyber security incident" is a commission of an act against, or failure to protect, the Department of State's unclassified cyber infrastructure from potential damage or risk.

12 FAM 592.1 Cyber Security Infractions

(CT:DS-116; 11-01-2005)

a. A "cyber security infraction" is one subset of a cyber security incident that contravenes computer security policy but does not result in damage to State's cyber infrastructure. Cyber security infractions are often committed inadvertently. However, even inadvertent lapses or errors bear reporting because they may indicate the presence of an intrusion and unauthorized use. An unauthorized user can:

(1) Introduce malicious material;

(2) Commit fraud;

(3) Disrupt service in the Department's network; or

(4) Compromise the confidentiality of sensitive information.

b. Below is an all-inclusive list of incidents that would be considered cyber security infractions and put the data or the system at risk:

(1) Disclosure of non-public key infrastructure (PKI) user access passwords:

(a) Passwords authenticate valid AIS users.

(b) Disclosing passwords defeats accountability by permitting an unauthorized user to assume access for which there is no attribution. For example, an authorized method of granting another employee access to your email account (when required) is to use the "permissions" function rather than sharing your user account passwords.

(2) Attempts by a user to obtain unauthorized access;

(a) User accounts and data folders are protected to ensure confidentiality, availability, and integrity of the incorporated data.

(b) Access to a particular folder is determined by the data folder owner and/or granted by the system manager when it is created (e.g., users attempting to access another user's data files within a data folder, for which an access restriction has been imposed).

(3) Unauthorized transfer of electronic data from unclassified systems to classified systems;

(a) Writeable disks and optical media that have been inserted in or connected to unclassified systems may not be inserted in or connected to classified systems without specific authorization.

(b) The systems manager may authorize data transfers from unclassified to classified systems on a case-by-case basis if:

- The unclassified media is checked for viruses

- The media is cleared for use
- The action is documented

(4) Accessing improper Internet sites or services;

(a) Employees may use the Internet in moderation, on personal time, for matters that are not directly related to official business. However, certain personal uses of U.S. Government equipment and networks are strictly prohibited, regardless of whether the use occurs on or off U.S. Government premises or whether the use is during or outside normal work hours. These include purposely visiting sites as personal activities and:

- Incurring additional expenses to the U.S. Government
- Generating income for oneself or for an organization with which the employee is affiliated other than the Department
- Viewing sexually explicit material, gambling, or for the purposes of conducting unlawful or malicious activities, impact negatively on user productivity and the integrity, accessibility and confidentiality of the Department's cyber infrastructure

(b) Purposely visiting these sites will be deemed, at a minimum, a cyber security infraction. If the visitation was inadvertent or unintentional, such activities will not be deemed a cyber infraction (see 12 FAM 592.2 (2) for a description of how this type of incident could be elevated to cyber security violation).

(5) Failure to remove a Type 2 crypto module (i.e., PKI smart card token) from an individual workstation or server that is logged on; and

(a) Keeping the PKI token (on "the smart card") inserted in an unattended AIS or server that has not been logged off could allow unauthorized users to impersonate the rightful user; and

(b) Undermine relationships of professional trust

(6) Disclosure of a PKI password.

(a) Disclosing PKI passwords permits an unauthorized user to enter into a confidential relationship with an unsuspecting employee.

(b) Falsely authenticating unauthorized users can enable them to mimic true users by falsely signing with digital signatures with access to such Sensitive But Unclassified (SBU) information as:

- Medical records
- Personnel files
- Financial information meant for official use only

12 FAM 592.2 Cyber Security Violations

(CT:DS-116; 11-01-2005)

a. A "cyber security violation," the second subset of a cyber security incident, is more serious than an infraction. It results in damage or significant risk to the Department's cyber infrastructure due to an individual's failure to comply with established Department computer security policy.

b. Below is an all-inclusive list of incidents that will be considered cyber security violations:

(1) Deliberate introduction of malicious program code;

(a) Malicious program code (i.e., viruses, worms, Trojan Horses, and scripts) can deliver sophisticated attacks that spread rapidly throughout the Department's AIS causing damage to its cyber infrastructure, disrupting critical activities and the Department's mission requirements.

(b) Excising viruses often involves shutting down the network, disrupting operations and incurring significant costs.

(c) The Department attempts to protect the network from malicious program code by vigorously applying patches, managing firewalls, employing automatic virus protection, etc.; however, this only protects the network from previously identified threats.

(d) Users must also share in this responsibility by strictly

adhering to the Department's computer security policy. Failure to perform mandatory virus scans of electronic media introduced into the network via an auxiliary drive, opening suspicious attachments to emails from unknown senders, or downloading software/tools from known hacker websites will be considered a deliberate act of non-compliance.

(2) Accessing improper Internet sites or services;

(a) Employees may use the Internet in moderation, on personal time, for matters that are not directly related to official business.

(b) Certain personal uses of U.S. Government equipment and networks are strictly prohibited, regardless of whether the use occurs on or off U.S. Government premises or whether the use is during or outside normal work hours (see FAM 592.1b(4) for an explanation of what personal uses are prohibited). If a pattern of such activity is established, or if this incident results in damage or significant risk to the network, it will be deemed a cyber security violation.

(3) Achieving or providing unauthorized administrator-level access;

(a) Achieving or providing unauthorized administrator-level access affords the recipient unfettered access to restricted information and system security configuration and controls; and

(b) Compromises the integrity of the cyber infrastructure.

(4) Use of PKI to conceal an unauthorized act;

(a) Use of encryption to hide an unauthorized action, such as the transfer of SBU to an unauthorized individual, is an abuse of PKI privileges.

(b) It demonstrates the sender's intent to conceal the unauthorized transmission.

(5) Introduction of unauthorized Type 2 cryptography;

(a) Unauthorized Type 2 cryptography refers to commercially available encryption software that enables the user to send information through the Department's network to another user with the same software bypasses system security configuration standards.

(b) The Department's PKI is the only Type 2 cryptography that may be operated on the Department's networks.

(6) Obtaining unauthorized user-level access;

(a) Intentionally gaining unauthorized user-level access (e.g. receiving, pilfering, or obtaining another's password through social engineering) violates at a minimum, the integrity of the system security controls.

(b) It could also result in the loss of the resident information's confidentiality, integrity and availability.

(c) Users gaining access to another user's data files (e.g. hacking into a data folder for which an access restriction has been imposed, puts the data and the system at risk).

(7) Defeating or attempting to defeat security seals on Department information technology (IT) devices;

(a) Security seals are placed on Department electronic devices to provide the user and the Department reasonable assurance that no unauthorized person has tampered with the device.

(b) Defeating or attempting to defeat the security seal renders the device unverifiable from a security standpoint.

(8) Defeating or attempting to defeat internal security measures of a Type 2 crypto module (PKI smart card token);

(a) Defeating Type 2 cryptography internal security measures may enable user access into areas where they are not authorized.

(b) That could enable someone to assume another's identity, compromising the integrity of the Department's information and systems.

(9) Deliberate installation of software not authorized by one of the Department's IT Change Control Board or Local Change Control Boards (IT CCB or Local CCBs);

(a) Installation of executable software containing a virus or other malicious code could compromise the confidentiality, integrity and availability of the network as well as the resident data.

(b) To prevent this type of compromise, all software must be examined/tested and authorized by the Department's IT CCB or local CCBs.

(c) Systems administrators may install specialized software necessary for performing official business, but only after the IT CCB or local CCB approved the software for use on Department AISs.

(10) Connection of prohibited hardware or electronic devices to Department AISs;

(a) The Department goes to great lengths to manage its cyber vulnerabilities and inoperability issues with its vast array of computer equipment.

(b) Installing unauthorized computer equipment, such as routers, switches and modems, can defeat the system's established security measures, thus putting the system at risk.

(11) Allowing unauthorized access or malicious modification to certificate authority servers, hardware cryptographic modules or registration authority workstations;

(a) Unauthorized access to or malicious modification of this system's security equipment subverts PKI functions necessary to ensure its confidentiality, integrity and availability.

(b) For example, unauthorized access or malicious modification can invalidate electronic signatures and deny cryptographic services.

(12) Installation of non-PKI hardware or software to certificate authority servers, cryptographic modules or Registration Authority workstations; and

(a) Installing unauthorized hardware or software to these systems can facilitate surreptitious system control.

(b) That can subvert the system manager's ability to assign and monitor the cryptographic and digital signature functions.

(13) Non-compliance with critical security configuration guidance.

(a) The Chief Information Officer (CIO) establishes a system

configuration guidance that allows system managers and other information system security activities to conduct critical monitoring functions. That protects the networks from intrusions and other malicious activities.

(b) Deviations from configuration guidance, unless specifically authorized by the CIO, could impair the Department's ability to secure its cyber infrastructure. If a need arises, IRM/IA, on behalf of the CIO, may waive configuration standards on a case-by-case basis.

12 FAM 592.3 Reporting Cyber Security Incidents

(CT:DS-116; 11-01-2005)

a. General: Due to the nature of the cyber incidents that are reportable in (see 12 FAM 592), most cyber incidents will surface as a result of a routine AIS security inspection or the Department's extensive network monitoring program. The primary intent of this program is to quickly detect incidents and take immediate action to control the possibility of damage to or repair the network, so the ISSO is an important link between the monitoring program and the Cyber Security Incident Program. The ISSO is responsible for notifying IRM/IA and the CIRT (DS/CS/MIR).

b. At posts abroad, the ISSO and regional security officer (RSO) must closely coordinate reporting of cyber security incidents in order to share relevant information. The RSO is responsible for conducting the investigation, with the technical assistance of the ISSO, to include the completion, processing and submission of the requisite security incident program reporting documentation (see 12 FAM 550).

c. Domestically, the bureau security officer (BSO) or DS/IS/APD will conduct the investigation with the assistance of the CIRT and/or servicing ISSO. It must include the required security incident program reporting documentation (see 12 FAM 550).

12 FAM 593 EVALUATION OF CYBER SECURITY INCIDENTS

(CT:DS-116; 11-01-2005)

a. DS/IS/APD performs evaluation and adjudication of all reported cyber security incidents to determine:

(1) The validity/invalidity of reported incidents;

(2) Whether they are infractions or violations;

(3) Whether further action is required; and

(4) Who is responsible for culpability for the incidents.

b. Employees will be held accountable for their individual actions.

(1) If supervisors are aware of subordinates committing cyber security incidents and allow the conduct to continue, they may also be held responsible for failure to provide effective organizational security oversight.

(2) This might occur, for example, when a supervisor allows subordinates to connect unauthorized hardware to the network or install privately owned software on U.S. Government computers.

c. When the investigation of a cyber security incident does not warrant charging a specific individual, DS/IS/APD may still adjudicate the incident as valid without holding a specific individual accountable.

(1) Mitigating factors may prevent narrowing responsibility to an individual employee or person; and

(2) The DS/SI/IS Office Director must approve this type of adjudication.

d. Upon completion of the adjudication, DS/IS/APD will notify in writing the culpable individuals charged during the investigation of the adjudication results specific to them. DS/IS/APD will also notify the appropriate RSO, BSO, or principal unit security officer (PUSO), who will provide a copy to the individual's supervisor.

12 FAM 594 APPEALS

(CT:DS-116; 11-01-2005)

a. An employee may appeal the validity or category (infraction versus violation) of a cyber security incident by submitting the appeal, in writing, to DS/IS/APD. This appeal request must be done immediately after receiving written notification that DS/IS/APD has adjudicated the incident.

NOTE: An employee's statement on Form OF-118 is considered part of the

initial adjudication, and does not initiate an appeal.

b. DS/IS/APD will forward the appeal, along with any other pertinent data, to the DS/SI/IS Office Director for a final appeal decision.

c. This appeal is exclusive and no further recourse may be had to any other forum.

12 FAM 595 ADMINISTRATIVE ACTIONS

12 FAM 595.1 Record Keeping and Administrative Action Framework

(CT:DS-116; 11-01-2005)

a. DS/IS/APD will maintain cyber incident investigations and adjudications files and documentation on all personnel, who have incurred cyber security incidents. Information from these files will be made available to the Director General of the Foreign Service and Director of Human Resources (M/DGHR) or other appropriate State Department officials with a need-to-know, as may be needed for deliberation of nominations or other personnel decisions. It will be included in full field investigation reports on candidates for Presidential appointments, and may be disseminated to relevant others consistent with the Privacy Act and other governing law. Upon an employee's termination, the records will be retired.

b. Cyber security incidents referred to the Bureau of Human Resources (HR) for disciplinary action will be handled on a case-by-case basis, but, in principle, disciplinary action will become progressive following additional incidents.

c. An employee's adverse cyber security incident history may result in the curtailment of a current assignment or denial of future assignments.

12 FAM 595.2 Referral for Disciplinary Action Related to Cyber Security Infractions (Department Employees)

(CT:DS-116; 11-01-2005)

Infractions: The following is a schedule of actions that will be taken for each infraction during the 36-month window:

(1) First infraction—The DS/IS/APD Division Chief will send a letter of warning to the employee that requires a signed reply from the employee acknowledging that he or she understands the policies and ramifications of future security incidents;

(a) The supervisor of the employee must provide counseling to the employee stressing the seriousness of the Department's cyber security policies.

(b) The ISSO and RSO or post security officer (PSO) abroad, or BSO/USO domestically, will provide the employee with remedial instruction and advice regarding cyber security.

(2) Second infraction—The DS/IS/APD Division Chief will send a letter of warning to the employee that includes a statement concerning actions DS will take in the event of future cyber security infractions;

(a) This warning notification requires a signed reply from the employee acknowledging that he or she understands the policies and ramifications of future security incidents.

(b) The ISSO and RSO or PSO abroad, or BSO/USO domestically, will provide the employee with remedial instruction and advice regarding cyber security.

(3) Third infraction—Letter of Caution. The DS/SI Senior Coordinator for Security Infrastructure will send a letter of caution to the employee that includes a statement concerning the actions DS will take in the event of future cyber security infractions.

(a) The letter of caution requires a signed reply from the employee acknowledging that he or she understands the policies and ramifications of future incidents.

(b) The system manager will suspend the user's AIS access until the ISSO retrains and retests the user on proper AIS procedures

(4) Fourth infraction—After affirmative adjudication and determination that a fourth and subsequent infraction within the 36-month window has occurred, DS/IS/APD will assign culpability.

(a) DS/IS/APD will then refer a Report of Investigation to HR/ER for appropriate disciplinary action (see 3 FAM 4300 and 3 FAM 4500) that includes:

- The current infraction and all previous infractions within the same 36-month window
- Any mitigating or aggravating factors
- Other cyber and information security incidents

(b) DS/IS/APD will forward referrals for disciplinary action of locally employed staff (LES) (when authority for that remains at post) to the RSO for delivery to the HR office at post.

(c) For cleared personnel, DS/IS/APD will refer the matter to the Director of the Office for Personnel Security and Suitability (DS/SI/PSS) for appropriate action to be taken relating to their security clearances.

(d) The system manager will suspend the user's AIS access until the ISSO retrains and retests the user on proper AIS procedure.

12 FAM 595.3 Referral for Actions Related to Cyber Security Violations (Department Employees)

(CT:DS-116; 11-01-2005)

a. After affirmative adjudication by DS/IS/APD that a cyber security violation has occurred and culpability is assigned, DS/IS/APD will refer the report of investigation to DS/SI/PSS and HR/ER for appropriate action. It must include a summary of mitigating or aggravating factors, and a list of other cyber and information security incidents (see 3 FAM 4300 and 3 FAM 4500).

b. DS/IS/APD will forward referrals for disciplinary action of locally employed staff (LES) (when authority for that remains at post) to the RSO for delivery to the HR office at post.

c. The system manager will suspend the user's AIS access until the ISSO retains and retests the user on proper AIS procedure.

12 FAM 595.4 Referral for Actions Related to Cyber Security Incidents (Other Agencies' Employees)

(CT:DS-116; 11-01-2005)

a. Cyber security incidents involving employees of other Federal agencies or organizations or their contractors are reported in the same manner as described herein (see 12 FAM 592). RSOs and ISSOs abroad must coordinate reporting all such incidents, including processing Form OF-117, Notice of Security Incident, and Form OF-118, Record of Incident, to DS/IS/APD. DS/IS/APD will coordinate any further investigation.

b. The system manager will suspend the user's AIS access upon each occurrence of a cyber violation as well as the third and subsequent infractions in a 36-month window until the ISSO retrains and retests the user on proper AIS procedure.

12 FAM 595.5 Referral for Actions Related to Cyber Security Incidents (Contractors)

(CT:DS-116; 11-01-2005)

a. DS/IS/APD will forward copies of Form OF-117 and Form OF-118 and the documented results of any investigation to the contractor's facility security officer for appropriate action and to the Office of Information Security, Industrial Security Division (DS/IS/IND).

b. DS/IS/IND will advise the Department's contracting officer representative (COR) of the nature and seriousness of the incident, and will provide details of any derogatory information to the cognizant security clearance investigative authority.

c. The system manager will suspend the user's AIS access upon each occurrence of a cyber violation, and also for the third and subsequent infractions in a 36-month window, until the ISSO retrains and retests the user on proper AIS procedure.

12 FAM 596 CRIMINAL LAWS

(CT:DS-116; 11-01-2005)

Incidents involving intentional risk or damage to U.S. Government AISs may be subject to criminal penalties.

12 FAM 597 THROUGH 599 UNASSIGNED